

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF NEW YORK

SUSAN B. LONG,  
DAVID BURNHAM, and  
TRAC REPORTS, INC.

Plaintiffs,

v.

U.S. IMMIGRATION AND CUSTOMS  
ENFORCEMENT, and  
U.S. CUSTOMS AND BORDER  
PROTECTION,

Defendants.

Civil Action No.: 5:23-cv-01564  
(DNH/TWD)

**DECLARATION OF HEATHER LYNCH**

**HEATHER LYNCH** declares the following under the penalties of perjury:

1. I serve as the Cybersecurity Risk Management and Assessment (CRMA) Branch Chief within the Office of the Chief Information Officer (OCIO) for U.S. Immigration and Customs and Immigration Enforcement (ICE) within U.S. Department of Homeland Security (DHS). I am responsible for maintaining ICE information security governance, enterprise risk management, and compliance with federal regulations including the Federal Information Security Modernization Act (FISMA). In summary, the function of ICE OCIO's mission is to provide infrastructure, governance, incident response capabilities, and oversight to deliver mission capabilities securely, efficiently, and effectively. Prior to joining ICE, I served as the CISO and Chief Privacy Officer of the National Technical Information Service (NTIS). As such, I make this declaration based on my personal knowledge, training, and experience as well as information provided to me by other ICE employees in the course of my official duties and my review of

records kept by ICE in the ordinary course of business. I make this declaration in support of ICE's Motion for Summary Judgment in this case.

2. As explained below, Plaintiffs' FOIA request presents an unacceptable risk of exposing individuals' identities and subjecting individuals and demographically identifiable groups to significant civil, privacy, social, psychological harms and potentially life-threatening security risks. Specifically, Plaintiffs' FOIA request would present risks to migrants, migrants' relatives and associates, government personnel, attorneys, witnesses, and other communities.

### **PLAINTIFFS' FOIA REQUEST**

3. I make this Declaration in response to the Plaintiffs' proposal submitted on August 1, 2024, which I have been told is the operative FOIA request for these purposes. In the August 1, 2024, letter, Plaintiffs request that ICE produce the following three subsets of records from the EID:

- a. "All datapoints (from any time) that are directly or indirectly linked to a person for whom the Agencies have established an official case seeking that person's removal from the country." ("Part 1").
- b. "All datapoints (from any time) that are directly or indirectly linked to a person who was apprehended pursuant to a Customs and Border Protection (CBP) 'encounter' in or after Fiscal Year 2020, with 'encounter' used to mean the same thing that CBP uses it to mean in its Nationwide Encounters Dataset." ("Part 2").
- c. "All code files, lookup tables, or other records that translate the specific codes used in connection with the datapoints contained in paragraphs (1) and (2) above into their corresponding meaning." ("Part 3").

**PLAINTIFFS' REQUEST FOR EID DATA INCLUDES THOUSANDS OF POTENTIAL  
DATAPOINTS OF PERSONAL INFORMATION, SENSITIVE PERSONAL  
INFORMATION, AND DEMOGRAPHICALLY IDENTIFIABLE INFORMATION  
ABOUT INDIVIDUALS THAT COULD BE USED TO REIDENTIFY INDIVIDUALS**

4. The EID contains thousands of datapoints about any given individual. Therefore, as explained below, even if a person's name has been removed from the EID data, there is a high risk that disclosing the data Plaintiffs seek would enable a third party to connect the data to an individual. Once the data is connected to an individual, any number of sensitive details about a person present in the EID data would be available to the third party, or if the third party chose to make the information public, to the public at large. This process is known as re-identification. To use a familiar and simple example, the game *Guess Who* illustrates how a person (the "subject" in this example) can be re-identified using seemingly innocuous information. Each player starts looking to identify one subject out of twenty-four people. Each player therefore asks for basic—and seemingly innocuous—information, such as the color of the subject's eyes and the color of his/her hair. Each of these data points, *on its own*, seems harmless. However, when put *together*, the answers to these questions lead to the re-identification of the subject.

5. The EID data requested contains approximately 12,000 data fields directly or indirectly linked to a migrant's case, including extensive personal information (PI), sensitive personal information (SPI), and demographically identifiable information (DII). Each category of data will be explained in more detail in the coming paragraphs.

6. EID datapoints for any given record include thousands of pieces of PI: information that relates back to a specific natural person—as to migrants, their relatives, associates, and the professionals who engage a migrant's case over time. This PI includes information known as direct identifiers and indirect identifiers:

a. Direct identifiers, also referred to as personally identifiable information (PII), are data that a person can use to identify a person without any additional data. Examples of direct identifiers include full names, mobile phone numbers, social security numbers, and alien file numbers, as well as biometric identifiers (i.e. iris scans, fingerprints, genetic data). Phone numbers and social security numbers, for example, are unique and therefore even though the person's name is not disclosed by the information, once the number is looked up, the person's identity will be readily revealed.

b. Indirect identifiers are PI that can reveal a person's identity in combination with other data. Examples of indirect identifiers include gender, birth year, occupation, or country of origin. By way of illustration, while many people are born on a given day and therefore a date of birth alone is not a direct identifier, once more datapoints (like gender, occupation, and country of origin) are introduced, determining the person's identity quickly becomes easier. To use another example, while a job title itself is generally not a direct identifier, a person could be identified through a basic LinkedIn search, for example, when their first name, job title, and employer are combined.

7. The EID data requested also contains sensitive personal information (SPI): personal information whose disclosure could result in discrimination or impact the individual's rights, safety, opportunities, and social or psychological well-being. Common types of SPI include health information, race, ethnicity, criminal history, identification as a victim of crime, sexual orientation, gender identity, political affiliation, and religion. Revealing an individual's status as transgender, for example, could expose the person to social exclusion or workplace discrimination. Revealing an individual's status as a victim of rape could expose the individual to retribution or harassment.

8. Finally, the requested EID data includes demographically identifiable information (DII): data that can enable the identification and targeting of people based on demographic characteristics such as race, ethnicity, country of origin, or occupation. Imagine, for example, that a data set about a city's homeless populations revealed that homeless children ages 14-17 tended to reside in specific city blocks. Traffickers could use that information to groom homeless youth, a demographic group particularly vulnerable to trafficking and sexual exploitation.<sup>1</sup>

9. Plaintiffs' current request to ICE, and more specifically Part 1 and Part 2, seek "datapoints . . . that are directly or indirectly linked to a person." Plaintiffs therefore seek a multitude of PI, SPI, and DII which can be used to piece together someone's identity. If a third party achieves re-identification, all of this data would be available on any given individual within the dataset.

10. I understand Plaintiffs may seek to require ICE to use substitute identifiers in its production. The risk of re-identification persists even if ICE uses substitute identifiers for the people whose information exists within the database because of the sheer amount of data that would be disclosed about the individuals in the database.<sup>2</sup> Plaintiffs' request to preserve "relational information" (in their words) only increases the risk that a person can be re-identified using the datapoints within the EID because preserving "relational information" would link all the data to an individual in various ways, expressing the interconnections between the underlying data as related to an individual.

---

<sup>1</sup> Kyleigh Feehs & Alyssa Currier Wheeler, 2020 Federal Human Trafficking Report, Human Trafficking Institute (2021), available at <https://traffickinginstitute.org/wp-content/uploads/2022/09/2021-Federal-Human-Trafficking-Report-WEB-1.pdf>

<sup>2</sup> I understand providing substitute identifiers could become burdensome and time-consuming given the number of fields that could need to receive substitute identifiers and given that Plaintiffs seek to preserve "relational information" as they define that term.

11. De-identification, pseudonymization, and anonymization are common approaches used to protect data subjects' privacy and reduce risks of disclosing data subjects' identities.

a. **De-identification** is the removal or masking (i.e. changing how data is displayed) of direct identifiers. Although de-identification reduces the likelihood of immediately identifying a person, it does NOT prevent re-identification. In 2019, researchers at the Imperial College of London produced algorithms that could correctly identify 99.98% of Americans from any data set using only 15 basic demographic indirect identifiers.<sup>3</sup>

b. **Pseudonymization** is a form of de-identification that replaces a direct identifier (such as a full name) with a unique ID – i.e., a pseudonym – such as a random string of numbers. Pseudonymization is often used when re-identifying an individual is necessary or when different records about a person need to be linked while still masking data subjects' immediate identities. Pseudonymization does NOT prevent re-identification, and in many cases, is designed to enable re-identification.

c. **Anonymization** is the process of altering personal information so that a natural person's identity cannot be deduced. Anonymization is **irreversible**. Once a data set has been anonymized, individuals' identities cannot be pieced back together. Irreversibility is critical to protect individuals' privacy when re-identification could endanger people's safety, opportunities, and well-being. Data **can only be considered anonymized** when:

---

<sup>3</sup> Rocher, L., Hendrickx, J.M. & de Montjoye, Y.A. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun* 10, 3069 (2019). <https://doi.org/10.1038/s41467-019-10933-3>

- i. Sufficient actions (whether through data removal, obfuscation, masking, replacement, etc.) have been taken to prevent the identification of a natural person; and
- ii. The natural person(s) cannot be re-identified.

12. These re-identification concerns persist even if the data is pseudonymized or de-identified because of the amount of datapoints that would be available to use for re-identification.

13. The data would need to be anonymized to mitigate the risks of re-identification that disclosure poses here. But anonymizing the broad swath of data Plaintiffs seek is technically infeasible, if not practically impossible, due to the nature of the data requested and the changes in the data and technology landscape that make re-identification highly possible and likely as explained in the remainder of this Declaration. Further, to the extent Plaintiffs seek to have ICE produce the data with substitute identifiers, ICE would not be able to anonymize data at all. Finally, and independently, insofar as Plaintiffs seek to preserve “relational information” (which will link the datapoints to each other), even de-identified data would still be linked in various ways, which would increase the risk of re-identification.

**THE EID DATA PLAINTIFFS SEEK CONTAINS HIGHLY SPECIFIC, SENSITIVE, AND EVEN INTIMATE INFORMATION REGARDING MIGRANTS, THEIR FAMILIES, WITNESSES TO CRIMES, AND GOVERNMENT EMPLOYEES**

14. Plaintiffs have explicitly requested thousands of pieces of personal information. Although most of these data points link to individual migrants, some data also pertains to personal information about migrant family members and associates, government personnel and attorneys engaging a migrant’s case, and even witnesses of highly sensitive crimes.

15. By way of example, the EID documents nearly 20 million migrants' cases and contain more than 12,000 fields of data across roughly 1,000 tables. Nearly 75 percent of data fields (an estimated 9,000 fields) could be produced in relation to an individual migrant record based upon the request. An average case lasts just over four years but can extend beyond a decade. As a case extends, the number of data points collected about an individual increases. Cases may begin when a migrant is a newborn infant or involve young unaccompanied children. Approximately six percent of migrants in cases contained in the EID are minors at the point of removal.

16. These thousands of fields of personal information paint detailed pictures of migrants' lives, whereabouts, families, relationships, health, interactions with law enforcement, and in some cases, criminal histories. EID data includes demographic information such as race, birth year, marital status, occupation, gender, country of origin, country of birth, country of citizenship, weight, height, and hair color. The data also hold sensitive personal demographic information capturing ethnicity, religion, veteran status, gender/sexual identity, and whether the individual is transgender. Data contain SPI like personal health information (PHI), which can document migrants' health conditions, medical clearances, pregnancy status, and if a pregnant individual is nursing. Data can also contain highly intimate and sensitive information about physical disabilities, amputations, the presence of breast or penile implants, the bodily locations of scars, and moles, and detailed descriptions of tattoos.

17. Credible fear cases provide a crucially sensitive set of data because the data pertains to cases where there is a "significant possibility" that a migrant facing removal has "been persecuted or [has] a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion if returned to [their] country," or

where “it is more likely than not that [they] would be subject to torture if returned.”<sup>4</sup> The data also includes special vulnerability codes indicating if a migrant is seriously mentally ill, a victim of sexual abuse or a violent crime, disabled, at risk based on sexual orientation/gender, or otherwise exceptionally vulnerable. These data points represent remarkably sensitive personal information that if connected to an individual, could subject individuals to discrimination, exploitation, and potentially life-threatening persecution.

18. Another particularly sensitive set of cases involve children as young as newborns, which necessitate collecting children’s personal information. Cases may involve minors charged with crimes or affiliated with gangs, including minors who have fled cartels and have credible fears of retaliation. The EID data indicates if a child is a verified versus claimed minor, whether the child is separated from family, entered the United States as an unaccompanied minor, and where the child resides. Children’s personal information is inherently sensitive, as children, particularly young children, are less likely to understand the implications of data collection and sharing, and exercise limited autonomy and can be subject to specialized and heightened risks.

19. The requested records also feature robust location data pertaining to interactions with law enforcement, where an individual was at a given date and time, and where an individual lives or has lived. EID data can be used to track individuals’ points of departure, entry, re-entry, and apprehensions in the United States. Law enforcement booking records include precise GPS data. EID data may also include precise location descriptions (addresses, latitude and longitude coordinates) that can map migrants’ personal contacts and family networks.

---

<sup>4</sup> [Questions and Answers: Credible Fear Screening | USCIS](#)

20. EID data also contains location data regarding the whereabouts of migrants in government facilities and in alternatives to detention (ATD). For individuals residing in government facilities (i.e. detention centers, prisons, etc.), the EID contains highly specific data about the facility, including the location, type of facility, and information about the facility's capacity to house children (by sex) and other vulnerable populations. The EID even stores the person's location within a facility and identifies the specific cell a person is housed in. Children may reside in official facilities under ICE or even Office of Refugee and Resettlement (ORR) custody. For adults participating in ATD, EID records track the ATD residence, points of contact, and the method of monitoring (e.g. phone calls, GPS device, etc.)

21. Migrant cases involving criminal charges include highly detailed information regarding the criminal charges. Incidents are captured regardless of whether a charge is discontinued, a conviction is overturned, the migrant is convicted, or they are found not guilty. Charges range from misdemeanors like pickpocketing to more serious crimes like human trafficking. The EID data includes granular NCIC charge codes representing crimes ranging from purse snatching and selling marijuana to potentially controversial charges like military desertions, attacks against law enforcement officers, "abortal acts against oneself" or others, and sexual offenses. NCIC charge codes for sexual offenses describe acts as sensitive and specific as incest with a child, bestiality, and "sodomy against a girl with a weapon." The EID also stores granular information regarding vehicles and property seized in criminal incidents. Such data detail the precise locations where contraband is seized, the type of contraband, quantity, and other descriptors. As explained below, records detailing criminal incidents may include attorneys' and witnesses' personal information.

22. Additionally, the EID contains highly specific information about gang-affiliated migrants. The EID codes include more than 900 codes for unique gangs. The data also specify the individual's role in a gang and whether the individual has gang tattoos.

23. The EID dataset also extends to personal information about witnesses involved in specific criminal incidents, which is highly sensitive. For any given incident, witness information collected can include full names, whether the witness is alive or deceased, detailed physical descriptions (height, weight, race, complexion), birth date and year, sexual identity/gender, and country of citizenship. The presence of a witness, or any combination of this identifying information, may not be known to the subject or other interested parties. Records also mark whether the witness has information that may be relevant to federal investigations or if they may be called upon to testify in official court proceedings, which again may not be known to the subject or other interested parties. Any information entered about a witness is date and time stamped and related back to a specific incident whose records may include detailed information about a crime.

24. The EID also captures detailed information about a migrant's family members and points of contacts. The EID documents basic demographic information like marital status and the number of children a person has. It also captures whom the migrant entered the United States with, if they entered the United States with a member of their family unit, and if they have relatives in the United States. Unique family unit IDs link individuals to other family members whose cases are also captured in the EID; these family unit IDs are important for case management, but as discussed below, present nuanced privacy risks. Personal relationship records document individuals that the migrant has relationships with, categorize the nature of the relationship, and include contact phone numbers. Information captured at the point of detention includes detailed pocket trash records, including phone numbers found in the pockets of detainees' clothing.

25. The EID contains information about ICE, CBP, USCIS, and other DHS personnel, other government employees and law enforcement agents, and government contractors. The EID automatically records date stamps, time stamps, and user IDs—unique IDs identifying a single employee—every time an authorized user creates or updates an EID datapoint. The EID also shows what agency the user works at; such information is either explicitly displayed or can be determined.

26. The EID also includes personal information about other government officials engaging a migrant’s case that access the EID data. Data collected includes government employees’ first, middle, and last names, pay grades, job title, program area, and even the employee’s social security number. Detailed information about government contractors is also gathered, including names, salaries, job titles, work locations, and organizations.

27. The EID also captures information about law enforcement agents when a migrant is accused of assaulting an officer. In such incidents, the name of the officer attacked, type of attack (verbal, physical, etc.), injuries sustained, and the location of incident are documented.

28. The EID also contains information about attorneys representing and prosecuting a migrant’s case including attorneys’ first and last names, law firms, phone numbers, and attorney bar numbers. In some states (including New York), a third party can readily find an attorney’s address, phone number, and other personal information by searching by an attorney’s bar number.

**KNOWN RE-IDENTIFICATION METHODS COULD, AND DO, REASONABLY  
PRESENT RISKS OF RE-IDENTIFICATION TO INDIVIDUALS  
BY THIRD PARTIES USING EID DATA SOUGHT BY PLAINTIFFS**

29. Earlier, I briefly explained the concept of re-identification. I will now provide a more nuanced explanation of the techniques and the risks posed by those techniques. The techniques presented here are actual—in that the techniques have actually been used in prior, documented, incidents around the world—as opposed to theoretical. These techniques will

continue to be used (and indeed will be refined) in the future.

30. Advances in technology, combined with the proliferation of personal information in the internet age, have dramatically increased the feasibility of re-identification. Advanced analytic techniques currently allow any technically savvy third party to identify individuals even when direct identifiers have been stripped. Rapid enhancements in computational power make it easier and faster to re-identify people across disparate data sources and large-scale datasets, such as the EID data Plaintiffs seek here. Even without data science skills, any person equipped with internet access can use publicly available information or low-cost data broker subscriptions to identify people.

31. Entity Resolution (ER) is a broad subset of data science processes used to determine if different pieces of information describe the same person, location, or thing, even when that information is displayed differently across multiple data sets. ER techniques are wide-ranging and involve using algorithms (rules or calculations) to compare records and determine how similar the records are. When chained together, these methods could reasonably be (and indeed are) very effective at locating the most similar records across EID datasets to identify data that describe unique individuals (or individuals sharing a common trait), even when direct identifiers are stripped. For example, ER algorithms could also be used to predict whether subsequent or future records describe a unique person captured in existing data. Coupled with other information, then, ER algorithms would allow someone to put together a historical picture of ICE's activities with regard to a specific person.

32. The scale, scope, and historical nature of the requested EID data significantly enhance the feasibility of developing highly accurate ER algorithms. EID data includes nearly 20 million migrants' cases. A single case houses thousands and thousands of data points that can be connected to create intricate maps of a person's life and personal networks over multiple years. Skilled data scientists could easily exploit this robust data set to develop algorithms that could accurately re-identify individuals documented in existing and future records.

33. The first step in ER is to cleanse the data and prepare data to be compared across records and data sources. This may include case conversion (e.g., converting text to lowercase), punctuation removal, standardizing location information (e.g., 'ST' and 'STR' = 'STREET'), etc.<sup>5</sup> A missing value strategy could also be implemented dynamically. For example, geolocation tools can complete missing city and state information, and name modeling tools that leverage census data can complete country of origin for given names. These steps help to both enrich and create structure in the data, making records more robust for comparison. **Skilled data scientists could thus easily clean data from a plethora of external sources to compare external records with EID records as a part of gathering data and re-identifying subjects.**

34. After data is cleaned, various techniques can be deployed.

35. Blocking is the simplest ER technique for segmenting records into logical groups for comparison. A block is a subset of records whose features match one or more patterns. Key and token-based blocks match text or partial text (e.g., first three letters of the last name). A simple block could be created using just "Gender" and "Birth Country," producing a block for every unique combination of records that match on Gender and Birth Country (e.g. a unique block could

---

<sup>5</sup> If ICE disclosed the information sought in Part 3 of Plaintiffs' request, this process would either be completed for Plaintiffs or would be easily constructed.

involve all records where Gender = female and Birth Country = Ecuador). Sorted neighborhoods sort the dataset by variables of interest and use fixed windows (i.e., record counts) to define block size. Blocks can be created using any number of variables in the data, making them highly flexible. One could add additional variables to the example block above, and sort data into blocks based on Gender, Birth Country, Area of Arrest, and Gang Affiliation, for example. The resulting blocks define the list of initial potential matches within each group. Thus, blocking performs an important first pass over the data to ensure match candidates are only considered alongside those that share global features.

36. Blocking then enables similarity scoring, which can then be used to score, threshold, and rank EID records for match likelihood (i.e. the likelihood that any two records describe the same person). This can be done with a few features or the entire set, if desired (this highlights the importance of data enrichment as cleaner data will exhibit higher scores). These rankings serve as the basis for manually labeling a “truth set” of candidate matched pairs, where records describing the same person are merged into a single record. These single records are “truth records” within the “truth set.”

37. Data cleansing, blocking, and similarity scoring are powerful on their own, suggesting an initial set of candidate matches in the data. These strategies also enable more powerful re-identification tasks: clustering, label creation, and machine learning.

38. Clustering is a network analysis method for creating, visualizing, and analyzing nodes (records) in a network. Networks are defined by their cluster centers, and each node is assigned to a center based on a set of features (such as similarity scores). Two records that have a shared gang affiliation or a shared family member (even in the absence of a unique family unit code) will be numerically linked closer. In addition to being a visual aid for investigation, networks

can be scored, which makes them a useful tool for evaluating the strength of association within each cluster.

39. A “truth set” of consolidated records belonging to unique individuals is typically created after scoring and/or clustering. This is a set of manually labeled records the research team believes to be actual matches and/or non-matches. Truth sets yield labels/targets that can be used in machine learning algorithms.

40. Using the features of the dataset as inputs and the truth set labels as targets (outputs), machine learning models can learn what determines a likely match and make predictions about likely matches against future records. These models learn from the structure and content of the underlying data. Thus, the more consistent and voluminous the training data (i.e., repeated EID FOIA ingests), the easier it becomes to match otherwise disparate records.

41. The techniques described above may be effective when applied solely to EID data. However, they are likely enhanced with a dataset comprised of information from multiple sources across the web. Multi-source data include additional records and feature columns that serve to augment the EID data. The augmented data may have a more robust set of features, which would theoretically bolster the effectiveness of ER re-identification.

42. Finally, even down-sampling (reducing) the number of required FOIA records would likely have little impact on the Plaintiff’s ability to effectively re-identify individuals on a large scale. First, a sample of just ten percent still corresponds to over 20,000 records which is more than sufficient to achieve effective results via the methods described above. Second, the performance of machine learning models hinges on the volume, veracity, and recency of the underlying data. Even the most performant model may become stale over time, but the characteristic of novelty allows for updates to the internal structure (parameterization). When

combined with existing data, these new samples not only supplement the observable information, but they add this latent recency value that models can use to update the relative importance of the input features. Thus, even a redacted release contains useful data and metadata that would likely enrich an existing re-identification process.

43. Yet another concern is Open-Source Intelligence (aka OSINT), which involves analyzing information available to the general public. The breadth of personal information stored in the requested EID records, combined with highly specific auto-generated date and time stamp data make it extremely feasible to re-identify individuals captured in EID records through OSINT.

44. For the purposes of illustration, when provided with sample EID records, ICE cybersecurity personnel were able to re-identify individuals **stripped of full names and other direct identifiers** in just under an hour – simply by searching local city and state online public arrest records. ICE officers frequently pick up individuals from local jails and prisons when individuals are released. In such cases, the jail or prison notifies ICE of the release, and ICE asks the facility to hold the individual using a detainer. EID records contain precise detention dates, providing key information to search open records.

45. Even without detention dates, dates could be deduced based on date and time stamps that are automatically generated when detention records are first created. As explained above, EID records store precise booking information, including booking record date and time stamps, including the GPS location of booking events. If these EID records are released, individuals can be re-identified using open-source local prison and jail websites like <https://www.jailexchange.com/> that allow the public to search for inmates based on detention dates. State, city, and local jails and prisons store many dates such as booking dates, discharge dates, image dates of when the inmate's arrest public photo, and more.

46. Indeed, once the subject is re-identified by name, low-cost data broker sites that aggregate arrest records such as “Been Verified” could be used to search individuals by name, which would allow a third party to confirm the subject’s prior arrests, and get access to the other personal information, including the person’s phone number, current and previous home addresses, usernames, email, social media accounts, and the names and contact information of their family members. Simply stated, a motivated individual could use this information to track down someone and find out where they live in and execute attacks.

47. In sum, advances in technology would enable the technically savvy to leverage Entity Resolution to re-identify individuals, even if EID data is de-identified, and particularly if data is only pseudonymized. Meanwhile, the rapid evolution of the internet provides any threat actor with the ability to leverage OSINT to re-identify individuals. Changes in the digital landscape thus render the true anonymization of EID data practically impossible.

**COMPLYING WITH PLAINTIFFS’ FOIA REQUEST COULD REASONABLY PRESENT RISKS TO INDIVIDUALS AND GROUPS WHOSE IDENTITIES WOULD BE SUBJECT TO RE-IDENTIFICATION FROM EID RECORDS**

48. As explained in the preceding section, if ICE complies with Plaintiffs’ request, ICE would be providing data that could reasonably be used to expose the identities of migrants, their family members and associates, witnesses related to case investigations, government personnel, and professionals like attorneys involved in a migrant’s case.

49. As explained above, EID records contain substantial personal information that could reveal individuals’ identities and, conversely, that could expose highly sensitive information about an individual if re-identified. Further, as explained above, re-identification is extremely feasible using technical and non-technical approaches. The breadth and detail of personal information held in the EID, including precise location data, not only materially enhances the risk

of re-identification, but also the ability to physically locate people in and outside of detention, including now legal residents.

50. I would now like to draw attention to the severe real-world risks posed to migrants, witnesses, migrants' family members and associates, government officials, attorneys, and demographically identifiable communities.

51. Exposing nearly 20 million migrants whose cases are managed in the EID to re-identification presents extreme risks at an alarming scale. Risks posed to migrants are complex and varied, ranging from social exclusion and discrimination, psychological distress, political persecution, and assassination. This section provides only a subset of the vast array of harms releasing EID data poses.

52. The exposure of migrants' identities leaves individuals vulnerable to retaliation, exploitation, and other abuses by gangs, cartels, human smugglers, traffickers, other criminal entities, and even abusive spouses or family members. The EID houses information of significant value to criminal threat actors. For example, the EID captures an individual's gang affiliation, gang role, gang tattoos, criminal histories, and detailed information about criminal incidents and property seized by law enforcement. The EID dataset also provides precise information on where migrants are located, whether in jail, prison, detention facilities, in ATD, or otherwise. As mentioned above, records even identify the specific cells individuals in facilities dwell in. By leveraging techniques described above, criminal actors could identify, locate, and harm migrants in and out of detention.

53. Criminal organizations could reasonably be highly motivated to exploit EID data in a range of scenarios, including to:

a. Retaliate against, silence, or extort migrants suspected of colluding with law enforcement and aiding criminal investigations.

b. Punish individuals who compromise criminal operations. For example, EID records could expose that law enforcement seized significant quantities of narcotics from a migrant while intercepting a drug deal.

c. Attack or threaten members of rival gangs.

d. Identify other gang-affiliated members to engage in criminal operations with.

e. Threaten migrants who “owe” debts to human smugglers.

f. Target migrants to scam in acts of organized fraud.<sup>6</sup>

54. As explained above, there are numerous examples of SPI stored in the EID, ranging from transgender identity and ethnicity to highly specific crime codes, intimate health information, and indicators of special vulnerabilities. The EID dataset also includes credible fear cases, where migrants may be vulnerable to persecution or torture if returned to their home country. Risks to migrants whose SPI is exposed are multi-faceted, numerous, and severe. Scenarios of particular concern include:

a. Individuals with credible fear cases could face retaliation from their persecutors and their proxies inside the U.S. or if deported. Threats could range from kidnapping, assassination, physical and psychological torture, and similar acts of retaliation against one’s family members.

---

<sup>6</sup> Soregel, Alison A. “First nationwide study of scams targeting immigrants shows local social context may help or hinder reporting.” UC Santa Cruz. February 10, 2022. <https://news.ucsc.edu/2022/02/immigration-scam-reporting.html>

b. Individuals exposed as LGBT, particularly from communities where LGBT persons are persecuted, are vulnerable to social exclusion, harassment, deprivation of economic opportunities, and acts of physical violence.<sup>7</sup>

c. Exposing individuals' health information presents wide-ranging risks. Individuals exposed as having disabilities or mental health conditions could face discrimination, social exclusion, harassment, and online bullying.

d. Exposing individuals' criminal histories, even in cases where a person was found innocent, presents wide-ranging risks. For example:

i. Prior gang affiliation, regardless of whether a person remains affiliated, could prevent individuals granted legal residency from obtaining work and integrating into communities.

ii. Individuals suspected of child sexual abuse are susceptible to threats of violence inside and outside of prisons.

iii. Migrants associated with "abortional acts" could be targeted by politically motivated actors, harassed, and subject to physical and psychological harms.

55. Witnesses re-identified through the EID are exceptionally vulnerable to threats of retaliation. Witnesses captured in the EID include individuals called upon to testify in cases against highly organized and violent cartels, human traffickers, and smugglers. Organized crime groups are a key potential threat actor that would be motivated to re-identify and target witnesses. Criminal threat actors could leverage the EID data and open-source data to identify, locate, extort and

---

<sup>7</sup> Linares, Albinson. "LGBTQ migrants face 'triple vulnerability' as a group in Mexico aims to help them." NBC News. June 19, 2024. <https://www.nbcnews.com/news/latino/lgbtq-migrants-mexico-discrimination-violence-rcna157916>

threaten witnesses and their families. Such threats expose witnesses to serious psychological, emotional, and security harms. Threats against witnesses also hampers prosecutors' abilities to build, maintain, and effectively implement cases against organized crime groups.

56. The EID also contains significant personal information related to a migrant's family members and personal contacts. This data could be easily combined with external data sources to identify and locate a migrant's family members and associates, subjecting them to numerous risks.

57. First, criminal actors can exploit data to threaten a migrant's friends and family members in order to:

- a. Inflict retribution against migrants' family members as acts of revenge due to a migrant's affiliation with a criminal organization.
- b. Demand that a migrant's family members pay "debts" a migrant owes to human smugglers.
- c. Carry out threats against family members to assert control over a migrant and force the migrant to commit crimes.

58. The nature and structure of EID data also poses complex risks to family members that may be victims of a migrant's suspected or convicted crimes such as incest and domestic violence. The EID applies unique family unit IDs to link related individuals' cases and include codes categorizing how family members are related. Although these direct linkages are crucial for case management, their exposure also poses severe and complex psychological, social, and security harms.

59. Imagine, for example, that the EID captures an adult male suspected of incest and sodomy against a boy (per the case records' NCIC codes). That individual is also marked as a member of a unique family unit, including a male son whose case is also managed in the EID. The child is thus linked as the son of a parent who is suspected of child sexual abuse. Even without a family unit id, however, Entity Resolution techniques could easily match individuals to their family unit. If EID data is exposed, this child could be accurately identified as a victim of incest, but also falsely identified (e.g. perhaps the actual victim is the adult male's nephew). Either scenario could result in severe emotional and psychological harms, bullying and social exclusion, or even retaliation by the male adult abuser.

60. Alongside individual migrants, the release of EID data poses heightened risks to demographically identifiable migrant communities based merely on immigration status or any combination of shared characteristics such as country of origin, age, sex, and language.

61. EID data can be analyzed to pinpoint clusters of migrant communities that share demographic characteristics. Entity Resolution techniques like clustering, for example, could enable threat actors to identify clusters of migrants that share the same country of origin and reside outside of detention facilities within the same 5-mile radius. Threat actors of diverse motivations could use that same combination of data to execute attacks. Threats against groups of migrants could include:

a. Anti-immigrant individuals or groups could harass, attack, or carry out acts of domestic terrorism against a community of migrants belonging to a particular country of origin, such as recent threats of mass violence against Haitian immigrants in Springfield, Ohio.<sup>8</sup> Threat actors could easily exploit EID data to find and target unknown clusters of Haitian migrants across the country.

b. Members of one ethnic group could identify and target communities they have historical ethnic conflict with.

c. Traffickers could identify groups of migrants of a particular sex, age, language group, etc. to recruit into various forms of labor exploitation.

62. As explained above, EID data documents children's cases as young as newborns. Child migrants face unique vulnerabilities that make them especially susceptible to abuse:

a. Unaccompanied minors lack the protection of parental supervision. Children separated from guardians are especially vulnerable to long-term psychological stress. This combination makes unaccompanied children particularly vulnerable to abuse and exploitation.<sup>9</sup>

b. Minors fleeing gangs and cartels may be subject to attacks by members of a group they were once affiliated with or by rival groups.

---

<sup>8</sup> "What to know about the threats in Springfield, Ohio, after false claims about Haitian immigrants." September 17, 2024. <https://apnews.com/article/springfield-ohio-haitian-immigrants-threats-key-details-7594bae869fb05dc6f106098409418cc>

<sup>9</sup> UNICEF. "[Post-expert Consultation Brief:] The Sale and Sexual Exploitation of Children: Migration." 2020. <https://www.unicef.org/innocenti/documents/sale-and-sexual-exploitation-children-migration#:~:text=Their%20vulnerability%20is%20exacerbated%20by,to%20sale%20and%20sexual%20exploitation>

- c. Children are vulnerable to pressure to join gangs due to power differentials, particularly if the minor faces compounding risk factors (family instability, lack of parental supervision, poverty, etc.).<sup>10</sup>
- d. Children in migration are at particular risk of experiencing mental health challenges due to violence and instability experienced in their countries of origin, during migration, or due to instability in their current circumstances.<sup>11</sup>
- e. Multiple risk factors, including poverty, family instability, or separation from guardians leaves migrant minors vulnerable to child labor exploitation.<sup>12</sup>
- f. Migrant girls are particularly vulnerable to sexual abuse and trafficking both during and after migration.<sup>13</sup>

---

<sup>10</sup> A. Jud, E. Pfeiffer, M. Jarczok, Epidemiology of violence against children in migration: A systematic literature review, *Child Abuse & Neglect*, Volume 108, 2020,104634, ISSN 0145-2134, <https://doi.org/10.1016/j.chabu.2020.104634>.

<sup>11</sup> Lisa H. Jay Cox, et al. “Violence, Exposure, Posttraumatic Stress Disorder, and Depressive Symptoms Among Recent Immigrant Schoolchildren.” *Journal of the American Academy of Child & Adolescent Psychiatry*, Volume 41, Issue 9, 2002, Pages 1104-1110, ISSN 0890-8567, <https://doi.org/10.1097/00004583-200209000-00011>.

<sup>12</sup> United States Health and Human Services. “Departments of Labor and Health and Human Services Announce New Efforts to Combat Exploitative Child Labor.” February 27, 2023. <https://www.hhs.gov/about/news/2023/02/27/departments-labor-and-health-and-human-services-announce-new-efforts-combat-exploitative-child-labor.html>

<sup>13</sup> UNICEF. “[Post-expert Consultation Brief:] The Sale and Sexual Exploitation of Children: Migration.” 2020. <https://www.unicef.org/innocenti/documents/sale-and-sexual-exploitation-children-migration#:~:text=Their%20vulnerability%20is%20exacerbated%20by,to%20sale%20and%20sexual%20exploitation>

63. Children may reside in official facilities under ICE or even Office of Refugee and Resettlement (ORR) custody. In cases where an unaccompanied child resides with a sponsor, the residence address may also be captured in EID. Malicious actors could abuse EID data to identify facilities or towns where pockets of minors reside, including clusters of unaccompanied migrant children and children of a particular sex, age, country of origin, ethnicity, or gang-affiliation. A short list of examples of ways threat actors could use cluster analysis and the EID data to exploit children include:

- a. Traffickers could target geographical pockets of migrant girls to groom and coerce into sexual exploitation.
- b. Regionally and ethnically affiliated criminal organizations could target and recruit children of specific ethnicities or countries of origin.
- c. Labor traffickers could identify pockets of vulnerable and unaccompanied minors to recruit into labor exploitation on farms and factories.

64. Government personnel such as ICE and CBP officers, law enforcement agents, detention facility workers, and government contractors engaging a migrant's case are vulnerable to a range of criminally and politically motivated threat actors. Location data, automated time and date stamp data, official user IDs, employment information, and other detailed personal information outlined above equips threat actors to identify and locate personnel affiliated with investigations, removal actions, and other aspects of case management.

65. First, criminal actors could exploit EID data to identify government officials for a range of malicious purposes, including (but hardly limited to):

- a. Carrying out retribution against law enforcement agents who disrupted criminal enterprises.

- b. Targeting officers to coerce or bribe into obstructing active investigations or colluding with criminal organizations.
- c. Conducting counter-surveillance against agents investigating criminal networks.
- d. Identifying staff working in detention facilities and prisons to coerce or bribe in order to communicate with, or continue criminal operations with, detained or incarcerated migrants, including migrants with active gang affiliations.

66. Government personnel are also vulnerable to harassment and attacks by politically and ideologically motivated actors driven by a range of causes. Immigration is a highly controversial issue provoking varied fervent, and even radical, views. Government personnel could be targeted by a range of pro- and anti-immigration actors.

67. In 2023, two members of the 2<sup>nd</sup> American Militia, an armed citizen border patrol group, were federally indicted for conspiracy to murder U.S. Border Patrol officers that would thwart their plot to open fire on migrants crossing over the U.S. border. Before his arrest, militia member Bryan Perry used TikTok to accuse the CBP of treason for allowing illegal immigrants to enter the U.S. and claimed such treason warranted their deaths.<sup>14</sup>

68. In recent years, a politically motivated threat actor searched for, aggregated, and exposed (i.e. doxed) the identities of thousands of ICE personnel online. Such acts of doxing—the deliberate and malicious publishing of personal information on the internet—exposed ICE personnel and their family members to harassment and security threats. ICE has since been

---

<sup>14</sup> Department of Justice. “[Press Release] Militia Members Indicted for Conspiracy to Murder Border Patrol Officers and Attempted Murder of FBI Agents”. May 31, 2023. <https://www.justice.gov/usao-wdmo/pr/militia-members-indicted-conspiracy-murder-border-patrol-officers-and-attempted-murder>

authorized to remove employee information from the public federal registries to protect staff and their families against real, ongoing threats.

69. Like government personnel, attorneys representing and defending migrants' cases are vulnerable to a range of criminally and politically motivated threat actors. Attorneys involved in prosecuting criminal cases involving migrants are particularly at risk of attacks by criminal actors. EID data could be exploited to identify and target attorneys supporting active investigations before indictments even occur, as well as attorneys in ongoing, past, and current trials. Criminal actors may exploit EID data to:

- a. Carrying out retribution against attorneys who prosecuted cases against criminal groups.
- b. Threaten or intimidate attorneys supporting active cases.
- c. Attempt to bribe or corrupt prosecutors.

70. In recent years, judicial officials have faced increasing incidents of politically and ideologically motivated online harassment, doxing, and violent attacks.<sup>15</sup> Like government officials, attorneys are vulnerable to doxing and targeting by both pro and anti-immigration actors. In February 2024, U.S. Marshalls Director Ron Davis testified before Congress that threats against federal judges had doubled since 2021, consistent with wider trends of political violence targeting U.S. public officials. Davis described 'alarming' upticks in social media attacks against judicial officials and death threats against judges.<sup>16</sup>

---

<sup>15</sup> United States Court. "Judiciary Affirms Need for Bill to Protect Federal Judges." July 14, 2021. [Judiciary Affirms Need for Bill to Protect Federal Judges | United States Courts \(uscourts.gov\)](https://uscourts.gov/judiciary-affirms-need-bill-protect-federal-judges)

<sup>16</sup> Lindsey Whitehurst. AP News. "Threats to federal judges have more than doubled in 'alarming' spike, US Marshals director says." February 14, 2024. <https://apnews.com/article/threats-federal-judges-us-marshals-alarming-a6a5398d6d09cf057eb5317592c8d299>

## CONCLUSION

71. In sum, the breadth and scale of risks posed to migrants, migrants' families, witnesses, government personnel, and attorneys if ICE were to comply with the Plaintiffs' FOIA request are severe, life-threatening, and ultimately untenable. The grave harms posed to millions of individuals, including children and highly vulnerable groups, must be considered with utmost seriousness. These risks are not mitigated by pseudonymizing or de-identifying. Furthermore, anonymization, the only viable pathway to prevent exposing millions of peoples' identities, is practically impossible, particularly given Plaintiffs' insistence on preserving what they term "relational information."

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge and belief. Signed this 1st day of October 2024.

---

Heather Lynch